

Institut National des Télécommunications	Module : ISSR34 - Filtrage	
Domaine: Sécurité - 3^{ème} Année.	Responsable : Olivier Paul	
Durée: 2H00	Documents : Autorisés	Nombre de pages : 5 pages
NOM :	Prénom :	Note:

- L'épreuve comporte deux exercices.
- Le document est accompagné de quatre annexes:
 - Annexe 1: Article «Domain Name System - wikipedia» de 8 pages.
 - Annexe 2: trace d'une communication DNS obtenue avec ethereal.
 - Annexe 3: trace d'une communication DNS obtenue avec ethereal.
 - Annexe 4: Article «IP Tunneling Through Nameservers - slashdot» de 2 pages..

Exercice I : Filtrage et DNS

(12 points)

Lisez l'article en annexe 1 **si nécessaire** avant de répondre aux questions suivantes.

Une entreprise possède un réseau local qu'elle désire connecter à Internet. Le préfixe 193.128.155/24 lui a été attribué. Nous nous intéressons par la suite à la gestion du filtrage associé au service de résolution de nom utilisé par cette entreprise. **Les autres protocoles seront donc ignorés.**

L'entreprise désire utiliser un serveur de nom interne afin que les équipements internes puissent être accessibles par des clients externes. De cette manière les équipements internes peuvent également être nommés. Elle fait l'acquisition d'un nom du domaine "test.fr". Elle utilise la station d'adresse 193.128.155.12 comme serveur de résolution de nom pour ce domaine. Cette station ainsi que les serveurs accessibles depuis l'extérieur sont placés dans une DMZ. Cette station est donc utilisée:

- Par les clients internes comme "DNS resolver" pour résoudre les noms d'équipements externes.
- Par les clients externes et internes comme serveur de nom pour le domaine "test.fr" pour résoudre les noms de tous les équipements internes.

L'architecture de filtrage se fait au travers d'un routeur filtrant munis de 3 interfaces:

- Une interface (I1) est connectée au réseau du fournisseur d'accès.
- Une interface (I2) est connectée au réseau interne.
- Une interface (I3) est connectée à la DMZ.

Afin de créer les règles de filtrage on examine le trafic entre les équipements internes et la machine d'adresse 193.128.155.12 (trace en annexe 2) ainsi qu'entre cette machine et le reste de l'Internet (trace en annexe 3). Enfin des échanges entre des serveurs externes et le serveur de résolution de nom auront également lieu. Ceux-ci sont semblables à ceux observés en annexe 2. En dehors de ces trafics, il est à noter que certains autres types d'échanges ne sont pas mentionnés par soucis de simplification, on les ignorera dans les règles de filtrage.

I.1. Dessinez l'emplacement des différents éléments.

**Par la suite lors de l'écriture de règles de filtrage on donnera ces règles dans le format suivant:
Interface, Direction, Protocole, Adresse Src, Port Src, Adresse Dst, Port Dst, Drapeaux, Action**

I.2. Donnez les règles de filtrage pour les trois interfaces en fonction du trafic observé en annexe 2.

I.3. Donner les règles de filtrage pour les trois interfaces en fonction du trafic observé en annexe 3.

Le serveur de nom permet également par défaut et au travers de requêtes similaires:

- à des clients d'obtenir le nom associé à une adresse (requête inverse)
- à des serveurs externes de réaliser des transferts de zone permettant de récupérer l'ensemble des informations concernant le domaine interne.

I.4. Vis à vis de ces points, cette architecture peut elle poser de problèmes de sécurité ? Pourquoi ?

Plusieurs solutions existent pour résoudre ce problème. Elles se basent généralement sur l'utilisation de deux serveurs DNS:

- Un premier serveur 193.128.155.12 est placé dans la DMZ de l'entreprise.
- Un second serveur 193.128.155.76 est placé dans le réseau interne.

On suppose par la suite qu'une telle architecture est utilisée.

I.5. Donnez la fonction de chacun des deux serveurs.

I.6. Donnez les règles de filtrage pour les trois interfaces.

Exercice II : Filtrage et Tunnelling

(8 points)

Lisez l'article en annexe 1 **si nécessaire** avant de répondre aux questions suivantes.
Lisez l'article en annexe 4 avant de répondre aux questions suivantes.

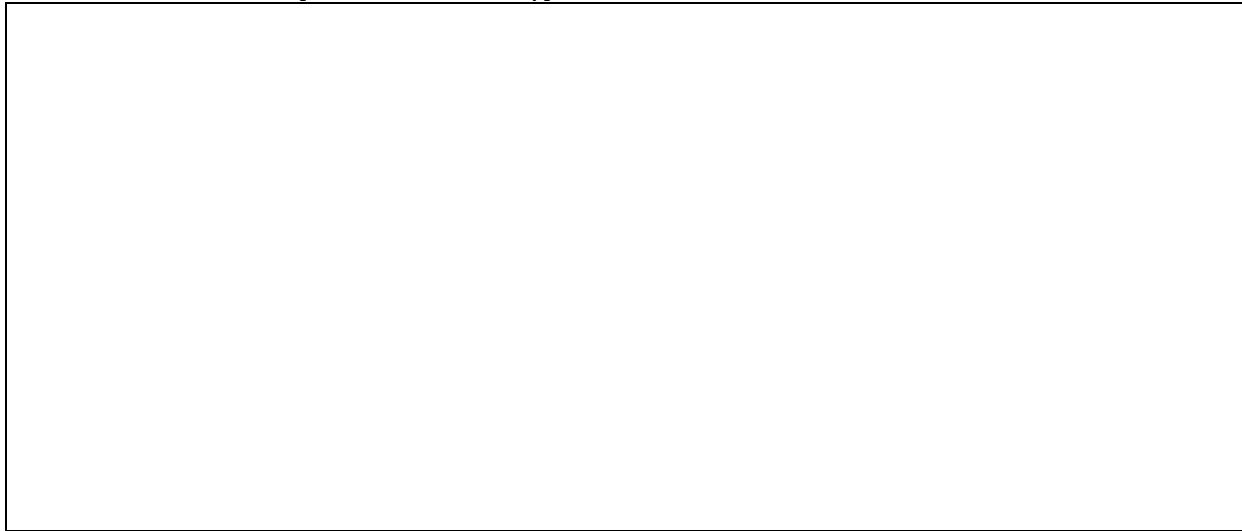
Une entreprise possède un réseau local qu'elle désire connecter à Internet. Le préfixe 193.128.155/24 lui a été attribué. Nous nous intéressons par la suite à la gestion du filtrage associé au service de résolution de nom utilisé par cette entreprise. Celle-ci utilise la station d'adresse 193.128.155.12 comme serveur de résolution de nom interne pour ce domaine.

On suppose que certains des utilisateurs internes du réseau 193.128.155/24 veulent utiliser le procédé indiqué en annexe 4 afin de faire ce qu'ils veulent sur Internet sans se préoccuper des règles de filtrage de leur administrateur réseau.

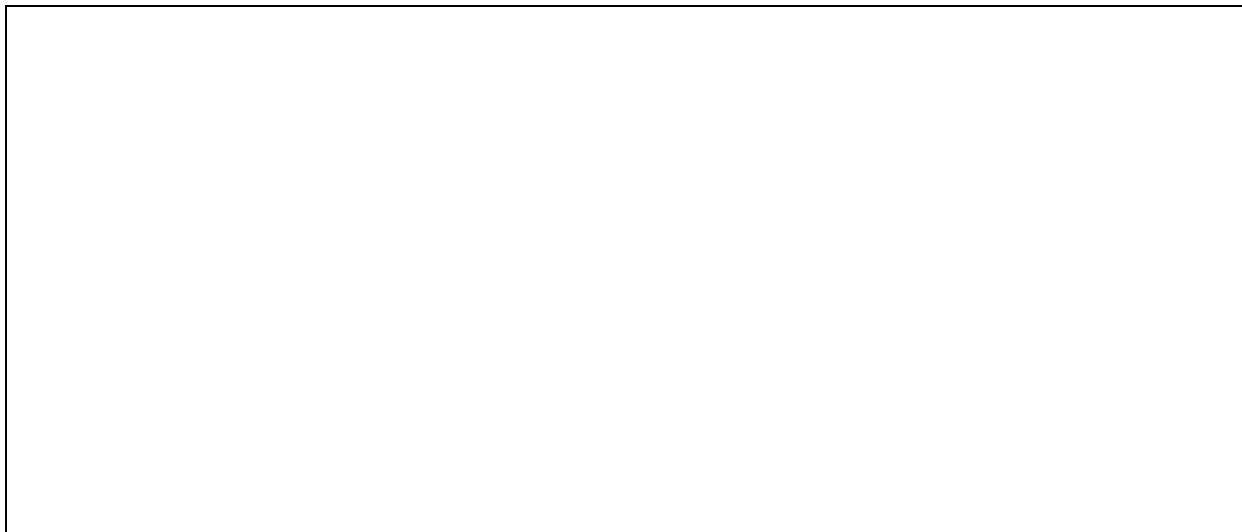
II.1 Comment le transfert des informations est-il réalisé entre les deux bouts du tunnel ?

II.2. Peut-on empêcher la création de ce type de tunnel sachant que les utilisateurs doivent accéder à des sites externes à l'entreprise ?

II.3. Peut on limiter le risque de création de ce type de tunnel au travers d'un filtre avec état. Comment ?



II.4. Peut on limiter le risque de création de ce type de tunnel au travers d'un filtre de niveau applicatif ?
Comment ?



II.5. Voyez vous un autre moyen de limiter ce risque ?

